IN THE CLAIMS

Claims 34 and 35 were added. Claims 32 and 33 have been cancelled. Claims 8, 9, 10 – 13, 16, 18, 19, 21 – 22, 24 – 25, and 27 have been amended.

Claims 1 – 7 (cancelled).

8. (currently amended) A computing system for performing a decryption operation on an encrypted packet, comprising:

a network driver to regulate said decryption operation and to transmit a decryption command;

a host memory to store the encrypted packet ~~after receipt by the computing system~~;

a controller to receive the encrypted packet and to perform said decryption operation after receiving said decryption command from the network driver;

a network interface to specify an ~~average~~ interrupt handler latency value to the controller, the interrupt handler latency value being based on a number of bytes of the packet upon which an action has been performed; and

a bus providing electronic communication among said network driver, said host memory and said controller, said controller asserting an interrupt ~~prior to a complete transfer of said decrypted packet from said controller to said host memory, wherein the controller waits the average latency value before said assertion of the interrupt in response to said decryption command~~ after the interrupt handler latency value has been occured and before the decrypted packet has been transferred back from the controller to the host memory.

9. (currently amended) The computing system of claim 8, ~~wherein said~~

~~computer~~ further includes a network interface to provide electronic communication between said ~~computer~~ computing system and a network.

10. (currently amended) The computing system of claim [[9]] 8, wherein ~~at least one security association (SA) is stored in said host memory~~ wherein said interrupt handler latency value is based on a specific number of bytes that have been transferred to the controller from the host memory and the interrupt is asserted after the specific number of bytes have been transferred to the controller.

11. (currently amended) The computing system of claim [[10]] 8, wherein said ~~network driver parses said encrypted packet, matches said encrypted packet with one of said at least one SA and instructs said controller to transfer said encrypted packet and said one SA across said bus to said controller~~ interrupt handler latency value is based on a specific number of bytes being decrypted in the controller and the interrupt is asserted after the specific number of bytes have been decrypted in the controller.

12. (currently amended) The computing system of claim [[8]] 10, ~~wherein said network interface includes a cryptography accelerator~~ wherein said interrupt is asserted before the encrypted packet is completely transferred to the controller.

13. (currently amended) The computing system of claim 8, wherein said ~~controller transfers said decrypted packet across said bus from said controller to said host memory~~ interrupt handler latency value is based on a specific number of bytes being transferred back to the host memory and the interrupt is asserted after the specific number of bytes have been transferred back to the host memory from the controller.

Claims 14 and 15. (cancelled)

16. (currently amended) A method of decrypting an encrypted packet received by a computing system, comprising:

receiving said encrypted packet from a network and transferring said encrypted packet to a host memory;

issuing a decryption command to a controller;

specifying an ~~average~~ interrupt latency value to the controller, the interrupt handler latency value being based on a number of bytes of the packet upon which an action has been performed;

~~waiting the average latency value before said assertion of an interrupt in response to said decryption command;~~

transferring said encrypted packet to said controller;

converting said encrypted packet to a decrypted packet; and

transferring said decrypted packet to the host memory; wherein [[the]] an interrupt is asserted ~~at a time before completing said transfer of said decrypted packet to said host memory~~ after the interrupt handler latency value has occurred and before the decrypted packet has been transferred from the controller to the host memory.

17. (cancelled)

18. (currently amended) The method of claim 16, wherein said ~~step of converting said encrypted packet to said decrypted packet further includes:~~

~~parsing said encrypted packet;~~

~~matching said encrypted packet with a corresponding security association (SA) stored in said host memory; and~~

~~transferring said encrypted packet and said corresponding SA to a controller~~

interrupt handler latency value is based on a specific number of bytes that have been transferred to the controller from the host memory and the interrupt is asserted after the specific number of bytes have been transferred to the controller.

19. (currently amended) The method of claim 16, wherein said ~~step of converting said encrypted packet to said decrypted packet further includes authenticating said decrypted packet~~ interrupt handler latency value is based on a specific number of bytes being decrypted in the controller and the interrupt is asserted after the specific number of bytes have been decrypted in the controller.

20. (cancelled)

21. (currently amended) The method of claim [[16]] 18, ~~further including indicating said decrypted packet to a protocol stack after asserting said interrupt~~ wherein said interrupt is asserted before the encrypted packet is completely transferred to the controller .

22. (currently amended) A program code storage device, comprising:

a machine-readable storage medium; and

machine-readable program code, stored on the machine-readable storage medium, the machine-readable program code having instructions that when executed cause a computer system to:

receive said encrypted packet from a network and transfer said encrypted packet to a host memory;

issue a decryption command to a controller;

specify an ~~average~~ interrupt latency value to the controller, the interrupt hanlder latency value being based on a number of bytes of the packet upon which an action has

been performed;

~~waiting the average latency value before said assertion of an interrupt in response to said decryption command;~~

transfer said encrypted packet to said controller;

convert said encrypted packet to a decrypted packet; and

transfer said decrypted packet to the host memory, wherein [[the]] an interrupt is asserted ~~at a time before completing said transfer of said decrypted packet to said host memory;~~ after the interrupt handler latency value has occurred and before the decrypted packet has been transferred from the controller to the host memory.

23. (cancelled)

24. (currently amended) The device of claim 22, wherein ~~said instructions to convert said encrypted packet to said decrypted packet includes instructions to:~~

~~parse said encrypted packet;~~

~~match said encrypted packet with a corresponding security association (SA) stored in said host memory; and~~

~~transfer said encrypted packet and said corresponding SA to a controller~~ said interrupt handler latency value is based on a specific number of bytes that have been transferred to the controller from the host memory and the interrupt is asserted after the specific number of bytes have been transferred to the controller.

25. (currently amended) The device of claim 22, wherein said ~~instructions to convert said encrypted packet to said decrypted packet includes instructions to authenticate said decrypted packet~~ interrupt handler latency value is based on a specific number of bytes being decrypted in the controller and the interrupt is asserted

after the specific number of bytes have been decrypted in the controller.

26. (cancelled)

27. (currently amended) The device of claim 22, ~~including instructions, which when executed cause the computing system to indicate said decrypted packet to a protocol stack after the instruction to assert said interrupt~~ wherein said interrupt handler latency value is based on a specific number of bytes being transferred back to the host memory and the interrupt is asserted after the specific number of bytes have been transferred to the host memory from the controller.

Claims 28 – 33 (cancelled).

34. (new) The method of claim 16, wherein said interrupt latency value is based on a specific number of bytes being transferred back to the host memory and the interrupt is asserted after the specific number of bytes have been transferred to the host memory from the controller.

35. (new) The device of claim 24, wherein said interrupt is asserted before the encrypted packet is completely transferred to the controller.